Department of Homeland Security Daily Open Source Infrastructure Report for 15 August 2007

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- USA TODAY reports a new flu vaccine plant is set to begin operations as soon as next year, boosting the supply of vaccine for the annual flu season and providing a much−desired U.S. source of vaccine for use in a flu pandemic. (See item 22)
- The Department of Homeland Security's Ready Campaign has released three new demonstration videos designed to highlight the specific steps older Americans, individuals with disabilities and special needs, and pet owners should take to prepare for emergencies. (See item 26)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 14, Associated Press* — **Colorado: Conference touts natural gas.** Energy industry officials from across the Rockies kicked off a three−day conference Monday, August 13, in Denver, by promoting natural gas, a cleaner−burning fossil fuel, as a weapon against increasing greenhouse gas levels. The annual conference by Denver−based trade group Colorado Oil and Gas Association opened with a panel discussion of climate change. Besides the normal industry discussions, four more sessions dealing with climate change and reducing carbon dioxide emissions were scheduled Tuesday and Wednesday. Fred Julander, of Julander Energy Co. and

the trade group's conference chairman, acknowledged the public's heightened concern about climate change and believes the gas industry should tout its advantages as a cleaner−burning fuel. Companies using new technology to tap the Rockies' vast reserves of gas in more environmentally sensitive ways can lead the way as the nation looks at reducing greenhouse gases, he added. Burning natural gas emits about half the carbon dioxide of coal and about a quarter the carbon of petroleum, according to the federal Energy Information Administration.
Natural Gas Conference: http://www.coga.org/frame/
Source: http://biz.yahoo.com/ap/070814/co_gas_conference.html?.v=1

2. *August 14, Platts Energy Bulletin* — **OPEC says 'emerging uncertainties' cloud oil demand outlook.** The Organization of the Petroleum Exporting Countries (OPEC) on Tuesday, August 14, raised its forecasts of world oil demand and demand for its own crude this year and next, but warned that the demand outlook was being clouded by a number of "emerging uncertainties." In its August Monthly Oil Market Report, OPEC's Vienna secretariat raised its forecasts of demand for crude produced by its own member countries to 31 million barrels per day (b/d) this year, 220,000 b/d higher than the 30.78 million b/d previously projected. But while it has revised the 2008 call on its crude upward by 50,000 b/d to 30.76 million b/d, it now sees demand for OPEC oil falling by 240,000 b/d year−on−year. These projections are significantly higher than the 30.38 million b/d OPEC estimates its members to have produced in July.
Report: http://www.opec.org/home/Monthly_Oil_Market_Reports/2007/mr0 82007.htm
Source: http://www.platts.com/HOME/News/8204851.xml?sub=HOME&p=HOME/News&?undefined&undefined

3. *August 14, Associated Press* — **Anniston Depot reported stolen radioactive devices.** Alabama's Anniston Army Depot reported the theft of two telescopes containing radioactive material days before reporting a small warehouse fire involving the same material. The Anniston Star reports that Nuclear Regulatory Commission (NRC) records show the two unconnected events were the first involving the Army Depot since 2000. An NRC spokesperson said depot officials followed the correct procedures. According to the EPA, tritium is one of the least dangerous radioactive materials. The Depot reported the theft of the two telescopes used on Howitzers, an artillery weapon, on August 2. They were found to be missing the week of July 23.
Source: http://beta.abc3340.com/news/stories/0807/447123.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *August 10, Associated Press* — **Federal workers evacuated during Hazmat spill.** The federal General Services Administration says three buildings and 150 people were evacuated for three hours Friday morning, August 10, after a small chemical spill at the Lakewood Federal Center in Colorado. Spokesperson Ben Gonzales said no one was hurt, and all the buildings have reopened. He said 30 gallons of hydrogen peroxide spilled at in a water treatment unit.
Source: http://www.kktv.com/coloradonews/headlines/9095676.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *August 14, Sophos* — **Facebook ID probe shows 41 percent of users happy to reveal all to potential identity thieves.** Sophos is warning social networking users of the dangers of allowing strangers to gain access to their online profiles, following new research into the risks of identity and information theft occurring through Facebook. Compiled from a random snapshot of Facebook users, Sophos's research shows that 41 percent of users, more than two in five, will divulge personal information to a complete stranger. To coincide with the research, Sophos has also published a best−practice user guide for behaving securely on Facebook. The Sophos Facebook ID Probe involved creating a fabricated Facebook profile before sending out friend requests to individuals chosen at random from across the globe. To conduct the experiment, Sophos set up a profile page for "Freddi Staur," a small green plastic frog who divulged minimal personal information about himself. Sophos then sent out 200 friend requests. "Freddi...encouraged 82 users to hand over their personal details on a plate," said Graham Cluley, senior technology consultant at Sophos.
   Facebook best−practice user guide:
   http://www.sophos.com/security/best−practice/facebook.html
   Source: http://www.sophos.com/pressoffice/news/articles/2007/08/face book.html

6. *August 13, ComputerWorld* — **Unusual pump−and−dump spam run continues.** More spam made its way to in−boxes Monday, August 13, touting a small Florida company first hit by a massive "pump−and−dump" scam last week. The company has denied any responsibility for the junk mail that drove up its stock price and said it will look at stockholder data in the hope that it can uncover who was behind the scheme. Prime Time Group Inc., a Ft. Lauderdale, FL−based company that owns and operates convenience and wireless stores in the U.S. and Caribbean, was the focus of a huge spam dump early last week that broke single−day records at several mail−filtering vendors. It appears that this pump−and−dump surge isn't over. "We saw a substantial uptick over the weekend, with the messages in FDF files, not PDF," said Ron O'Brien, a Sophos senior security analyst. The new spam created another spike in the share's price. On Monday, it hit nine cents early, a penny, or 12.5 percent, increase from Friday's eight cents, then swung several times before falling to near seven cents by 4 p.m. EDT. "This is one of the few times where a pump−and−dump has been sustained," O'Brien said.
   Source: http://www.computerworld.com/action/article.do?command=viewA rticleBasic&articleId=9030469&pageNumber=1

7. *August 10, Department of Justice* — **Man sentenced to seven years for identity theft and fraudulent use of thousands of credit and debit card numbers.** United States District Judge David C. Bury sentenced Jacob Vincent Green−Bressler of Tucson, AZ, on Friday, August 10, to 84 months in prison for his role in a criminal conspiracy, the object of which was the theft and fraudulent use of credit and debit card numbers and their associated personal identification

numbers. On March 9, 2007, Green−Bressler pleaded guilty to two felony offenses, conspiracy to commit offenses against the United States and aggravated identity theft, as well as a misdemeanor information charging possession of stolen authentication features. Green−Bressler solicited and was supplied with stolen credit and debit card account information of U.S. banking customers from individuals located in foreign countries, including Vietnam, Pakistan, Jordan, Egypt, Philippines, Macedonia, Romania, Estonia, Kosovo, Canada, Russia, United Kingdom, Panama, Morocco, Lebanon, Mexico, Australia, Lithuania, and France. Green−Bressler obtained this credit and debit card account information by visiting Internet Relay Chat rooms and forums run by the suppliers, as well as by private electronic messaging with these suppliers.
Source: http://www.usdoj.gov/usao/az/press_releases/2007/2007−182(Gr een−Bressler).pdf

8. *August 10, Finextra (UK)* — **Man−in−the−middle phishing kits circulating freely on the Web.** Security vendor RSA is reporting an increase in the amount of free "man−in−the−middle" phishing kits −− designed to subvert bank two−factor authentication controls −− circulating in the scammer underground. In its monthly online fraud report, the RSA FraudAction Intelligence team has highlighted a rise in the number of hacker repositories dedicated to providing free man−in−the−middle kits. The kits themselves target more than ten of the world's leading financial institutions, says the vendor. The free kits are usually primed to send stolen user credentials to both the instigator of the fraud and the creator of the software. The vendor first encountered demo kits for sale on the Web in January this year. It forecasts a sharp increase in man−in−the−middle attacks as the software becomes more widely available over the next twelve months.
Source: http://www.finextra.com/fullstory.asp?id=17300

9. *July 13, Government Accountability Office* — **GAO−07−769: Small Business Administration: Additional Measures Needed to Assess 7(a) Loan Program's Performance (Report).** The Small Business Administration’s (SBA) 7(a) program, initially established in 1953, provides loan guarantees to small businesses that cannot obtain credit in the conventional lending market. In fiscal year 2006, the program assisted more than 80,000 businesses with loan guarantees of nearly $14 billion. This report examines (1) the program’s purpose, based on its legislative history, and performance measures; (2) evidence of constraints, if any, affecting small businesses’ access to credit; (3) the types of small businesses served by 7(a) and conventional loans; and (4) differences in SBA’s estimates and reestimates of the program’s credit subsidy costs. The Government Accountability Office (GAO) analyzed agency documents, studies on the small business lending market, and data on the characteristics of small business borrowers and loans. GAO recommends that SBA take steps to ensure that the 7(a) program’s performance measures provide information on program outcomes. In written comments, SBA agreed with the recommendation in this report but disagreed with one comparison in a section of the report on credit scores of small businesses with 7(a) and conventional loans.
Highlights: http://www.gao.gov/highlights/d07769high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−769

[Return to top]

Transportation and Border Security Sector

10. *August 14, Associated Press* — **Chinese bridge collapse kills 28.** At least 28 people were killed after a bridge under construction in a popular Chinese tourist town collapsed as more than 100 workers were removing scaffolding, the government said Tuesday, August 14. So far, 86 people had been rescued, including 22 who were injured when the bridge spanning the Tuo River in central China's Hunan province collapsed Monday, the official Xinhua News Agency said. Five were in critical condition. The cause of the collapse of the 880−foot bridge was under investigation, the Hunan Administration of Work Safety said in a statement posted to the official Gov.cn Website. Premier Wen Jiabao ordered a thorough investigation into the accident, China Central Television reported. The 140−foot−high bridge in Hunan's Fenghuang county was scheduled to open at the end of this month, the administration said. Construction accidents in China are frequent, with contractors often opting for shoddy materials to cut costs and using migrant laborers with little or no safety training.
Source: http://www.usatoday.com/news/world/2007−08−14−china−bridge_N .htm?loc=interstitialskip

11. *August 14, Reuters* — **Russia train blast is terrorism.** Russia launched a terrorism investigation on Tuesday, August 14, after a bomb derailed an express train traveling from Moscow to St Petersburg, overturning cars and injuring dozens of passengers. "The train accident was caused by a homemade explosive device," Sergei Bednichenko, chief prosecutor for Russia's North West district, told Channel One television. "A criminal case has been opened under article 205, clause 3, that is terrorism." The head of Russia's Federal Security Service, Nikolai Patrushev, linked the bombing to an insurgency in the south of the country around Chechnya, where Moscow has been fighting a long rebellion against its rule. The derailed train was an overnight service traveling on one of the country's busiest rail routes. It is heavily used by businesspeople and foreign tourists. Sixty passengers and train crew were injured in the derailment, and 38 of them were admitted to hospital, a spokesperson for rail operator Russian Railways said. About 250 people were on board.
Source: http://www.cnn.com/2007/WORLD/europe/08/14/russia.train.reut /index.html

12. *August 14, Los Angeles Times* — **U.S. Customs agency in LAX snafu criticized.** Aviation officials criticized U.S. Customs on Monday, August 13, for being unprepared and taking too long to fix the weekend computer failure at Los Angeles International Airport (LAX) that left more than 17,000 international passengers stranded for hours in airplanes. Accustomed to frequent, short−lived outages, customs officials said they mistakenly believed their computers would be up and running within an hour Saturday, August 11. Then they made another mistake: they misdiagnosed the problem, deciding it involved high−speed communications lines that link to the national law enforcement databases used to assess possible security threats posed by arriving passengers. They called in the service provider, Sprint Nextel Corp. But a technician did not arrive for four hours, aviation officials said, and took three hours to determine that the transmission lines were not the problem. Paul Haney, deputy executive director for airports and security for Los Angeles World Airports, the agency that operates LAX, said customs notified airport officials of the problem about half an hour after it started. Soon, airport officials began setting up a crisis center as they considered options such as using schools to temporarily house incoming passengers who were technically not allowed to set foot on U.S. soil.
Source: http://travel.latimes.com/articles/la−me−laxairport14aug14

13. *August 14, Associated Press* — **Colorado Springs airport reopens after bomb threat, evacuation.** The Colorado Springs Airport was evacuated for about 2 1/2 hours Monday, August 13, after someone phoned in a bomb threat. The airport reopened at about 4 p.m. MDT after a search by officers and bomb−sniffing dogs turned up nothing, said John Leavitt, a spokesperson for the city, which owns the airport. At least four planes were diverted to other airports and other planes were held on the ramp at a safe distance from the terminal.
Source: http://www.aurorasentinel.com/main.asp?SectionID=11&SubSectionID=11&ArticleID=16820&TM=3467.851

14. *August 09, Associated Press* — **US Airways fires workers over false overtime.** US Airways Group Inc. said Thursday, August 9, it has fired 25 Philadelphia International Airport baggage handlers who falsified overtime records on the airline's computerized timekeeping system. More firings could be coming. US Airways said it is still in the process of interviewing about 100 to 150 people who may have been involved. The Tempe, AZ−based airline accused the employees of obtaining managers' computer passwords and altering records to make it look as if they had worked overtime when they did not, said spokesperson Andrea Rader. The system is being fixed to prevent another breach. US Airways has had severe baggage−handling problems in Philadelphia and starting last year hired hundreds of workers to manage increased traffic and offset employee turnover.
Source: http://biz.yahoo.com/ap/070809/pa_us_airways_false_ot.html?. v=1

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

15. *August 13, Agricultural Research Service* — **Fungus helps keep aflatoxin out of cotton.** In a brutal battle for food and space, two fungal cousins are currently duking it out across the nation's cotton fields. Thanks to biological control strategies developed by the Agricultural Research Service (ARS), the better of these two microscopic relatives is winning. While invisible and odorless, the Aspergillus fungi can churn out potent poisons called alfatoxins. These carcinogenic compounds −− linked to impaired growth, cancer and death −− would threaten human health if stringent food safety standards weren't in place to screen out contaminated products. When cottonseed becomes infested with toxin−making fungi, it must be discarded or severely downgraded. That's because the seed is a major feed of dairy cows, and any toxins that might be present could transfer to the animals' milk. Every year, aflatoxin is responsible for ruining three million to eight million dollars worth of cottonseed in the Southwest.
Source: http://www.ars.usda.gov/is/pr/2007/070813.htm

[Return to top]

Food Sector

16. *August 13, Nutra Ingredients* — **Salmonella fears for shark cartilage.** Batches of shark cartilage capsules originating from the U.S. could contain salmonella, the United Kingom Food Standards Agency has warned. The capsules, which are largely used for joint health, have been recalled by U.S. distribution firm NBTY which said it discovered the "issue" during routine testing of the product. While a routine test detected the bacteria, testing on additional batches of shark cartilage did not show any evidence of contamination.
Source: http://www.nutraingredients.com/news/ng.asp?n=78998−nbty−ftc −shark−cartilage

17. *August 13, Associated Press* — **State recalls smoked sausage.** New York State is warning people not to eat "Neparovana Smoked Sausage" sold at Muncan Foods in Ridgewood, Queens because of possible Listeria contamination. State Commissioner Patrick Hooker of the Agriculture Department says the "Neparovana Smoked Sausage" was sold bulk from the stores deli display cooler. State inspectors doing a routine sampling found the sausage contaminated with Listeria. No illnesses have been reported to date.
Source: http://www.1010wins.com/pages/802942.php?contentType=4&conte ntId=792975

18. *August 12, Intelligencer Journal (PA)* — **Salmonella warning issued.** Human cases of a rare type of salmonella illness have caused the Pennsylvania Department of Health to issue a warning to pet owners. The health department says 21 cases of the illness in Pennsylvania residents might be linked to dry dog food and advises using safe−buying and handling practices. The illness being investigated by the health department is caused by an uncommon strain of salmonella called schwarzengrund. Most of the infections occurred in households with pets or where people are in close contact with pets, but there is no evidence any human consumed pet food.
Source: http://local.lancasteronline.com/4/208026

[Return to top]

Water Sector

19. *August 11, New York Times* — **New York City fined over delay in water filtration project.** One of the costliest construction projects in New York City history, a $2.1 billion water filtration plant in the Bronx, is being fined $30,000 a day by the federal government because there is no primary contractor to start the work. For the past two years the city has been building, 100 feet below Van Cortlandt Park, the Croton Water Filtration Plant, which is scheduled to become operational in 2012. A large swath of the southeast portion of the park has been cleared of grass and trees, and digging is under way. But work on the filtration plant itself has not begun, officials said, even though the city was required by a federal court consent decree to hire a contractor for the job by February. Emily Lloyd, commissioner of the Department of Environmental Protection, said the complexity of the work was a major reason for the delays. “This is an enormous project and a very complicated process,” Lloyd said. “It was very difficult to site and design. It will be one of the largest filtration plants in the world.”
Source: http://www.nytimes.com/2007/08/11/nyregion/11plant.html?_r=3 &oref=slogin&oref=slogin&oref=slogin

20. *August 10, U.S. Environmental Protection Agency* — **EPA orders public water supply systems in Louisiana into compliance.** Based on numerous citizen complaints about the quality and safety of drinking water provided by public water supply systems in northeast Louisiana, the U.S. Environmental Protection Agency (EPA) announced the issuance of six administrative orders to owner/operator Jeffrey Pruett of West Monroe, Louisiana, for violations of the federal Safe Drinking Water Act. The public water systems subject to these orders are the Love Estates Water System, Cottonland Mobile Home Estates Water System, Charmingdale Subdivision Water System, Pine Bayou Water System, Lakeview Estates Subdivision Water System, and the Suburban North Subdivision Water System, all in the Monroe, LA, area. In July 2007, staff from the EPA Region 6 Public Water Supply Enforcement Team, along with staff from the Water Quality Protection Division and the Louisiana Department of Health and Hospitals (LDHH), inspected these water systems. Numerous operations and maintenance violations were found requiring immediate compliance action. These violations included improper storage of chlorine gas, insufficient chlorine residuals, unplugged abandoned wells, lack of a source of emergency electrical power, and no site security, among others.
Source: http://yosemite.epa.gov/opa/admpress.nsf/fdeef3661eb3b846852572a00065683e/606eb1b376d1108a85257333004c68d1!OpenDocument

[Return to top]

Public Health Sector

21. *August 13, Clarion−Ledger (MS)* — **Student OK after anthrax spill.** A graduate student at the University of Mississippi Medical Center broke a flask of anthrax cells on Saturday, August 11, in UMC's Biosafety Level 3 high containment labs where anthrax research is conducted. The student was treated as a precaution and permitted to go home.
Source: http://www.clarionledger.com/apps/pbcs.dll/article?AID=/2007 0813/NEWS/70813042

22. *August 12, USA TODAY* — **Vaccine maker gears up in case of flu pandemic.** A new flu vaccine plant is set to begin operations as soon as next year, boosting the supply of vaccine for the annual flu season and providing a much−desired U.S. source of vaccine for use in a flu pandemic. The $150 million plant was built by the French company Sanofi Pasteur on its 500−acre campus in the Pocono Mountains. It joins an older plant, built in the 1970s, that produces the only flu vaccine made entirely in the U.S. "We assume that in a pandemic, the only vaccine available to Americans is going to be a vaccine made in America," says Bruce Gellin, director of the National Vaccine Program office in the Department of Health and Human Services. "A goal of our pandemic vaccine program is largely to ensure we have sufficient domestic capacity to meet this country's need." Sanofi's existing plant, which is set to close down for renovations when the new plant goes online, churns out up to 50 million doses a year. The new one, which the company says will be ready in late 2008 or early 2009, will produce 100 million doses of vaccine for annual flu seasons.
Source: http://www.usatoday.com/news/health/2007−08−12−flu−vaccine_N .htm

[Return to top]

Government Sector

23. *August 13, KCCI (IA)* — **Suspicious package at University of Iowa destroyed.** A suspicious package forced the University of Iowa campus to evacuate two buildings on campus Monday, August 13. University employees discovered the package after receiving anonymous e−mails claiming four pipe bombs had been placed on campus. The suspicious package was found near Jessup Hall. The bomb squad destroyed it. Officials said the package did not contain any explosives.
Source: http://www.kcci.com/education/13883087/detail.html

[Return to top]

Emergency Services Sector

24. *August 14, Federal Emergency Management Agency* — **Hurricane Flossie update.** At 5:00 a.m. EDT, the center of Hurricane Flossie was located about 260 miles south−southeast of Hilo, HI, and about 455 miles southeast of Honolulu, HI. Flossie is moving toward the west−northwest near 15 mph and this motion is expected to continue overnight. Maximum sustained winds are near 115 mph with higher gusts. Flossie is a category three hurricane on the Saffir−Simpson scale. The Big Island will see the onset of tropical storm force winds 39 mph and higher directly associated with Hurricane Flossie mid−morning Tuesday, August 14. East to southeast winds of 40 to 50 mph with higher gusts are likely as Hurricane Flossie passes south of the Big Island during the day Tuesday. The Governor has declared a state of emergency. The proclamation allows the state and county governments to access the State Disaster Fund. It also allows the National Guard being preparations for any response they may be called upon to perform. The state is working with the Federal Aviation Administration and the airline carriers to ensure the customers are informed of what actions they must take to be safe and secure.
Source: http://www.fema.gov/emergency/reports/2007/nat081407.shtm

25. *August 14, Associated Press* — **Newark plans high−tech help for police.** The city of Newark, NJ, will be outfitted with high−tech cameras and other equipment to help police fight gun violence after the fatal shootings of three college students. The $3.2 million program includes gunshot detection technology to improve officer safety and increase neighborhood awareness. Mayor Cory A. Booker planned to announce details at a news conference Tuesday afternoon, August 14.
Source: http://hosted.ap.org/dynamic/stories/S/SCHOOLYARD_KILLINGS?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

26. *August 13, Department of Homeland Security* — **DHS releases new preparedness resources for seniors, people with disabilities, and pet owners.** The severe weather experienced this summer in parts of the country, and the continuing threat of terrorism, are reminders of how critical it is for all Americans to prepare for emergencies. The Department of Homeland Security's (DHS) Ready Campaign has released three new demonstration videos designed to highlight the specific steps older Americans, individuals with disabilities and special needs, and pet owners should take to prepare for emergencies. DHS worked with AARP, National

Organization on Disability, and The Humane Society of the United States to develop these new emergency preparedness resources. The videos remind individuals to get an emergency supply kit, make a family emergency plan, and be informed about the different types of emergencies while considering the unique needs of these individuals, their families, and caregivers. The videos recommend seniors include any necessary prescription medications in their emergency supply kits. It encourages Americans with disabilities or special needs to create a personal support network that they can rely on during an emergency. Pet owners are advised to learn which emergency shelters in their area and along their evacuation route will allow pets.
Source: http://www.dhs.gov/xnews/releases/pr_1187027722320.shtm

27. *August 13, York Dispatch (PA)* — **Database could save time, lives in emergencies.** People with physical or mental challenges could be targeted for quick evacuation during an emergency using a new tool York County, PA, is hoping to offer soon to municipalities. The county wants to help municipalities create databases of people who may need more help than others in an emergency, said Bruce Funk, assistant director of the York County Human Services Department. The databases could help first responders evacuate specific people, such as those with disabilities, in an emergency, he said. Responders could also get the people supplies if they are ordered to stay inside. Funk said municipalities would be responsible for compiling their own lists of people for the databases. However, the county is hoping to offer free or low−cost laptops with software they could use to compile them, Funk said.
Source: http://www.yorkdispatch.com/local/ci_6611900

[Return to top]

Information Technology and Telecommunications Sector

28. *August 14, IDG News Service* — **Nokia says 46 million batteries may overheat.** Nokia is offering to replace 46 million batteries made by another company for use in its mobile phones because of a risk of overheating, Nokia said on Tuesday, August 14. The faulty batteries were manufactured by Japan's Matsushita Battery Industrial Co. and sold in a wide range of Nokia phones, from its low−end 1100 family of products to its pricier N91 and E60 devices. Nokia said that in "very rare cases" a short circuit can cause the Nokia−branded BL−5C batteries to overheat while they are being recharged. It said it knows of about 100 incidents so far and that no serious injuries or property damage have been reported.
Source: http://www.infoworld.com/article/07/08/14/Nokia−batteries−ov erheat_1.html

29. *August 14, ComputerWorld* — **Record−breaking 'Storm' linked to spam surge.** Storm, the Trojan horse that hoovers PCs into hacker−controlled botnets, roared back into life last month in several waves, security researchers said Monday, August 13, and has blown by 2005's Sober to become the most prolific e−mail−borne malware ever. Thanks to Storm, MX Logic tracked a July jump in malicious e−mail of 1,700 percent over June. Storm, however, is much more malevolent than Sober. "Not only is it designed to propagate more copies of Storm, but it releases huge quantities of spam," said Sam Masiello, director of threat research at MX Logic Inc. Security analysts have been drawing a line between Storm's success and spam outbursts of July and August, including one that dropped impressive quantities of "pump−and−dump" stock scam mail in mailboxes worldwide.
Source: http://www.computerworld.com/action/article.do?command=viewA

rticleBasic&articleId=9030538&intsrc=hm_list

30. *August 14, Associated Press* — **Microsoft buys online−ad company.** Microsoft completed its $6 billion buyout of digital marketing company aQuantive Monday, August 13, and now plans to challenge Yahoo and Google in the online advertising business. Microsoft, which lags behind Yahoo and Google in search traffic and advertising revenue, is trying to shift toward offering software applications over the Internet.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/08/13/AR2007081300884.html

31. *August 13, InfoWorld* — **Novell buys endpoint security firm Senforce.** Novell announced on Monday, August 13, that it has acquired Senforce Technologies, a provider of endpoint and network security tools, for an undisclosed sum. Waltham, MA−based Novell also said that it would move quickly to integrate Senforce's technologies into its ZENworks product lineup in an effort to further expand its enterprise systems management offerings.
Source: http://www.infoworld.com/article/07/08/13/Novell−buys−endpoint−security−firm_1.html

32. *August 13, ComputerWorld* — **DirectX SDK bug means bad news for IE users.** The DirectX software development kit Microsoft issued in 2002 contains a critical vulnerability, a Polish researcher claimed as he released attack code that can hijack Windows PCs by tempting Internet Explorer (IE) users to malicious sites. According to Krystian Kloskowski, who posted exploit code on the milw0rm.com site, the FlashPix ActiveX control included with DirectX Media 6.0 SDK contains a buffer overflow bug that can be exploited. More importantly, according to an advisory issued by U.S. Computer Emergency Readiness Team (US−CERT) on Sunday, August 12, "because the FlashPix ActiveX control is marked 'Safe for Scripting,' Internet Explorer can be used as an attack vector for this vulnerability." IE 6 can be leveraged to exploit the flaw, noted Kloskowski, but he did not say if the newer IE 7 is also a workable attack vector.
US−CERT Vulnerability Note: http://www.kb.cert.org/vuls/id/466601
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9030418&intsrc=hm_list

33. *August 13, InformationWeek* — **Storm botnet behind Canadian DoS attack.** Researchers are blaming the virulent Storm worm for a widespread denial−of−service (DoS) attack that hit Canadian Websites over the weekend. The attack may have been unfocused and unsuccessful, but it could have been an early test of the DoS power that the Storm worm botnet now holds. Johannes Ullrich, chief research officer at the SANS Institute and chief technology officer for the Internet Storm Center, said in an interview that while sites in Canada were "pounded" over the weekend, he doesn't think it was a targeted DoS attack. The attacks weren't aimed at any particular Websites. It was just spread across a wide swath of the Internet.
Source: http://www.informationweek.com/software/showArticle.jhtml;jsessionid=M0HTKFZNYOS4CQSNDLRSKHSCJUNN2JVN?articleID=201500196

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

34. *August 11, The Mail (UK)* — **UK police on terror alert over theft of top secret records on computer database.** A major security alert in the UK has been sparked after the theft of a computer database containing thousands of top secret telephone records from police investigations into terrorism and organized crime. Worried police chiefs throughout the UK launched a massive inquiry into the removal of the sophisticated computer and other IT equipment from a private firm specializing in gathering evidence from mobile phone calls made by suspects. The raid at the high−security head office of Forensic Telecommunication Services Ltd (FTS) at Sevenoaks, Kent, raised fears that vital evidence from undercover investigations may have been lost or have fallen into the wrong hands. The stolen computer server contained details of who made calls on mobiles, their exact location and precisely when the calls were made. The computer server itself is of little or no monetary value. The value of the raiders' haul is the huge amount of data stored inside the equipment. The break−in last Monday night, August 6, is said to have caused "deep anxiety" among police forces in England and Wales, many of whom use the worldwide expertise of FTS in mobile phone analysis.
Source: http://www.mailonsunday.co.uk/pages/live/articles/news/news.html?in_article_id=474788&in_page_id=1770

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.

Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer